UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/017,392	12/18/2001	Yuusaku Ohta	2001_1828A	6503

513 7590 05/15/2006

WENDEROTH, LIND & PONACK, L.L.P.
2033 K STREET N. W.
SUITE 800
WASHINGTON, DC 20006-1021

EXAMINER	
TESLOVICH, TAMARA	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 05/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/017,392	OHTA ET AL.	
	Examiner	Art Unit	
	Tamara Teslovich	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02/23/06*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the Applicant's Remarks and Amendments filed February 23, 2006.

Claims 1-22 are pending and herein considered.

Response to Arguments

Applicant's arguments filed February 23, 2006 have been fully considered but they are not persuasive.

In response to pages 11-12 of the Applicant's Remarks concerning the Examiner's 35 USC 112 rejections of claims 1-22 as being incomplete for omitting essential structural cooperative relationships of elements and for failing to set forth the subject matter which applicant(s) regard as their invention, the Examiner maintains those rejections presented in the previous office action. Although the Applicant has provided an extensive explanation of how the authentication processing unit and the encryption processing unit operate in parallel and sequentially, a number of inconsistencies remain.

In pages 14-15 of the Applicant's arguments, the Applicant claims that claim 1 comprises "at least one authentication processing unit operable to perform the authentication processing in a data block of B2 bits in parallel to the encryption processing or the decryption processing performed by the at least one encryption processing unit". The Examiner has taken this argument, as well as those appearing further down on page 15 concerning the encryption processing of a B1 block parallel to the authentication processing of the B2 block, the B2

block comprising n B1 blocks, to mean that the parallel processing of claim 1 pertains to the encryption/decryption of a B1 block parallel to the authentication processing of a B2 block. It is unclear how the two processes could in fact be parallel considering the B2 block is in fact made up of n B1 blocks, which must go through the encryption/decryption unit before making it to the authentication unit. If it is the Applicant's intention to claim the encryption of a B1 block in parallel to the authentication of a B2 block, the B2 block not including the previous B1 block, it is imperative that the Applicant provide support for such limitations within the claim, including the necessary relationship between those B1 blocks and authentication values sent along to the packet construction unit to create a packet. At present, there is no relationship given between the B1 blocks and the B2 block authentication values sent to the packet construction units. For example, according to the invention as claimed, a packet can be constructed from a B1 block and the authentication value of a B2 block, that B2 block being unrelated to and not including the original B1 block. If it is the Applicant's intention to include within the final packet authentication values corresponding to those blocks included within the packet, the Applicant needs to amend the claims to include such a limitation.

The Examiner respectfully disagrees that the Applicant's amendments to claim 1 serve to clear up those objections presented in the previous office action. Although the Applicant has taken the necessary precautions to ensure that the newly added limitation differentiates between those blocks authenticated and those encrypted/decrypted, the Applicant has failed to amend the existing

limitations. Lines 8-12 of the Applicant's "Amendments to the Claims" included the previously presented limitation of:

> "at least one authentication processing unit operable to perform the authentication processing in a data block unit of B2 bits in parallel to the encryption processing or the decryption processing performed by said at least one encryption processing unit, and output the authentication value indicated the result of the authentication processing, the data block unit of B2 bits being n times the data block unit of B1 bits"

It remains unclear within this limitation how two processes may be performed in parallel wherein the secondary process utilizes the results of the first process in its calculations.

The Applicant's newly added limitation of:

> "wherein when the inputted packet is a packet which requires both encryption processing and authentication processing, the encryption processing of a first data block by said at least one encryption processing unit, and the authentication processing of a second data block by said at least one authentication unit are performed in parallel, the second data block to which the authentication processing is being performed being a data block which is different from the first data block and to which the encryption processing has already been performed by said at least one encryption unit and accumulated in said at least one data block accumulation unit"

to independent claims 1 and 18 fails to resolve those rejections previously presented regarding whether the authentication and encryption processes occurred sequentially or in parallel. The Applicant fails to provide a relationship between the B2 block and the B1 mentioned with respect to parallel processing and the 'first data block' and the 'second data block' of the newly added limitation and as a result it is unclear whether the parallel processing originally claimed is in fact the same parallel processing as that disclosed in the newly added limitation.

In response to the Applicant's arguments on pages 16-17 concerning Matthews' alleged failure to disclose a data block accumulation unit operable to accumulated data blocks to which the encryption processing has been performed, the Examiner respectfully disagrees and calls the Applicant's attention to paragraph 31 wherein it is discussed how once the data has been processed through the crypto engine, it is fed back to the authentication alignment block before being processed through the authentication component. The Examiner would also like to point to Figure 3 wherein it is clearly shown that the information coming from the crypto engine (358) is then sent (359) to the authentication alignment (304) to be collected and sent into the authentication engine (308).

In response to the Applicant's arguments concerning claim 2, and Matthews' alleged failure to disclose wherein both encryption and authentication processes are performed, the Examiner points to paragraph 30 wherein it is disclosed that that encryption alignment block and engine handle both encryption and decryption. The Examiner would also like to take a moment to note that although specific paragraphs have been referenced in this and previous office actions, those paragraphs were included to aid the Applicant in understanding the Examiner's rejections. However, the prior art of reference is to be considered in its entirety. In this specific situation, the Matthews reference is replete with mentions of the encryption of data followed by its authentication, beginning with the Abstract and continuing throughout the reference.

In response to the Applicant's arguments concerning claim 20 and Matthews' alleged failure to disclose wherein data blocks are able to bypass the accumulation unit resulting in high speed processing, the Examiner respectfully disagrees. First, the examiner would like to point out that the paragraphs cited by the Applicant, namely paragraph 24 and Figure 3, both make specific mention of the fact that they describe only a particular embodiment of the invention. Meanwhile, paragraphs 32-35 disclose how the alignment blocks are used according to the needs of the encryption being utilized. For example, Figure 5 shows the data aligned into six 32-bit rows representing three DES data blocks, but that depiction is only an aspect of the alignment logic available. The actual size and use varies with the particular encryption engine used. Also note paragraph 29 wherein it is taught that depending on the implementation of the authentication engine, processing may begin before the blocks are loaded.

In response to the Applicant's arguments concerning claim 21 and Matthews' alleged failure to disclose wherein data blocks are saved and restored via the data block accumulation unit, the Examiner respectfully disagrees and draws the Applicant's attention to paragraph 32 wherein a processing data saving unit is disclosed for temporarily saving the data blocks being processed to be utilized at a later time.

In response to the Applicant's arguments concerning claim 22 and Matthews' alleged failure to disclose wherein the suspended data blocks are passed on to another processor having equivalent functionality, the Examiner respectfully disagrees. The Examiner draws the Applicant's attention to

paragraph 35 wherein the prior art teaches saving blocks and passing them to units having the required functionality.

In response to the Applicant's final set of arguments concerning the patentability of claims 3-4, 7-8, 10-12, and 14-16 over Matthews in view of Videcrantz, the Examiner respectfully disagrees. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, it would have been obvious to a person of average skill in the area at the time of the invention to include within Matthews a control unit with the capabilities to determine which processing units have completed their calculations and are ready to output to the next processing unit as described in Videcrantz to in order to maintain order and expedite the time necessary to deal with incoming packets.

In view of the arguments previous, Examiner respectfully disagrees with the Applicant's argument that Matthews fails to disclose claims 1 and 18 in their entirety, and maintains the 35 U.S.C. 102(e) rejections corresponding to claims 1-2, 5-6, 9, 13, and 17-21 as well as the 35 U.S.C. 103(a) rejections corresponding to claims 3, 4, 7, 8, 10-12, 14-16 and 22 as recited below.

Claims 1-22 also remain rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential structural cooperative relationships of elements, such omission amounting to a gap between the necessary structural connections as set forth in previous office actions and explained above.

Claim Rejections - 35 USC § 102

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1, 2, 5, 6, 9, 13, and 17-21 are rejected under 35 U.S.C. 102(e) as being anticipated by Donald P. Matthews (U.S. Patent Application Publication 2002/0078342).

As per **claim 1**, Matthews discloses a security communication packet processing apparatus that performs at least one of encryption processing, decryption processing and authentication processing to a packet comprising

at least one encryption processing unit ("cryptography engine") operable to perform the encryption processing and the decryption processing in a data block unit of B1 bits (Matthews [0031]);

at least one authentication processing unit ("authentication engine") operable to perform the authentication processing in a data block unit of B2 bits in parallel to the encryption processing or the decryption processing by the encryption processing unit, and output an authentication value indicating the

result of the authentication processing, the data block unit of B2 bits being n times the data block unit of B1 bits (Matthews [0029]);

at least one data block accumulation unit ("authentication alignment block") operable to accumulate the data blocks to which the encryption processing is performed by the encryption processing unit, and, when the accumulated amount of the data blocks reaches B2 bits, output the data blocks to said at least one authentication processing unit (Matthews [0027]);

a packet construction unit operable to receive the encrypted or decrypted data blocks from said at least one encryption processing unit, receive the authentication value from said at least one authentication processing unit, and construct a packet including the received data blocks and authentication value (Matthews [0026]); and

a control unit operable ("cryptography alignment block") to divide the inputted packet into the data blocks of B1 bits, and output the data blocks sequentially to said at least one encryption processing unit (Matthews [0031]).

wherein when the inputted packet is a packet which requires both encryption processing and authentication processing, the encryption processing of a first data block by said at least one encryption processing unit, and the authentication processing of a second data block by said at least one authentication unit are performed in parallel, the second data block to which the authentication processing is being performed being a data block which is different from the first data block and to which the encryption processing has

already been performed by said at least one encryption unit and accumulated in said at least one data block accumulation unit (Matthews [0029-0031]).

As per **claim 2**, Matthews discloses the security communication packet processing apparatus according to Claim 1, wherein

said control unit is operable to judge whether the inputted packet is a first type packet requiring the encryption processing and the authentication processing, a second type packet requiring the decryption processing and the authentication processing, a third type packet requiring one of the encryption processing and the decryption processing, or a fourth type packet requiring the authentication processing only (Matthews [0011] reference 'distinguishes portions of non-pre-padded network security protocol packet requiring one and/or another operation - authentication and/or encryption" to permit single pass processing of data),

when said control unit judges that the inputted packet is the first type packet, said control unit is operable to divide the packet into the data blocks of B1 bits and output the data blocks sequentially to said at least one encryption processing unit (Matthews [0031]),

when said control unit judges that the inputted packet is the second type packet, said control unit is operable to divide the packet into the data blocks of B1 bits, output the data blocks of B1 sequentially to said encryption processing unit (Matthews [0031]), divide the packet or a duplicate of the packet into the data blocks of B2 bits, and output the data blocks of B2 bits sequentially to said at least one authentication processing unit (Matthews [0027]),

when said control unit judges that the inputted packet is the third type packet, said control unit is operable to divide the packet into the data blocks of B1 bits and output the data blocks sequentially to said at least one encryption processing unit (Matthews [0031]), and

when said control unit judges that the inputted packet is the fourth type packer, said control unit if operable to divide the packet into the data blocks of B2 bits and output the data blocks sequentially to said at least one authentication processing unit (Matthews [0027]).

As per **claim 5**, Matthews discloses a data path connection switching unit ("alignment logic configuration") operable to connect the output of the control unit and the input of the encryption processing unit, the output of the control unit and the input of the authentication processing unit, the output of the encryption processing unit and the input of the data block accumulation unit, and the output of the data block accumulation unit and the input of the authentication processing unit, respectively and independently (Matthews [0024]).

As per **claim 6**, Matthews discloses wherein said control unit is operable to judge whether the inputted packet is a first type packet requiring the encryption processing and the authentication processing, a second type packet requiring the decryption processing and the authentication processing, a third type packet requiring one of the encryption processing and the decryption processing, or a fourth type packet requiring the authentication processing only (Matthews [0011] reference 'distinguishes portions of non-pre-padded network security protocol

packet requiring one and/or another operation - authentication and/or encryption" to permit single pass processing of data),

when said consol unit judges that the inputted packet is the first type packet, said control unit is operable to control said data path connection switching unit so as to connect the output of the control unit and the input of said at least one encryption processing unit, the output of said at least one encryption processing unit and the input of said at least one data block accumulation unit, and the output of said at least one data block accumulation unit and the input of said authentication processing unit (Matthews [0031]),

when said control unit judges that the inputted packet is the second type packet, said control unit is operable to control said path connection switching unit so as to connect the output of said control unit and the input of said at least one encryption processing unit, and the output of said control unit and the input of said at least one authentication unit (Matthews [0027]),

when said control unit judges that the inputted packet is the third type packet, said control unit is operable to control said data path connection switching unit so as to connect the output of said control unit and the input of said at least one encryption processing unit (Matthews [0031]),

when said control unit judges that the inputted packet is the fourth type packet, said control unit is operable to control said data path connection switching unit so as to connect the output of said control unit and the input of said at least one authentication processing unit (Matthews [0027]).

As per **claim 9**, Matthews discloses a processing data saving ("memory") unit, for each of at least one of said at least one encryption processing unit, said at least one authentication processing unit and said at least one data block accumulation unit, each processing data saving unit having a memory area for temporarily suspending the processing of the data blocks in the processing unit for which said processing data saving unit and saving the data blocks which were being processed in the processing unit corresponding respectively to the processing unit (Matthews [0032]).

As per **claim 13**, Matthews discloses a processing data saving ("memory") unit for each of at least two said at least one encryption processing unit, said at least one authentication processing unit and said at least one data block accumulation unit, each processing data saving unit having a memory shared by the processing units for temporarily suspending the processing of the data blocks in the processing unit and saving the data blocks which were being processed in the processing units (Matthews [0032]).

As per **claim 17**, Matthews discloses wherein the B1 is 64 (Matthews [0027]), and the B2 is 512 (Matthews [0029]).

As per **claim 18**, Matthews discloses a security communication packet processing method that performs at least one of encryption processing, decryption processing and the authentication processing to an inputted packet, said security communication packet processing method comprising:

dividing the inputted packet into the data blocks of B1 bits (Matthews [0031]);

performing the encryption processing or the decryption processing to the divided data blocks of B1 bits (Matthews [0031]);

accumulating the encrypted data blocks and outputting the data blocks when the accumulated amount of the data blocks reaches B2 bits, B2 being n times the number of B1 bits (Matthews [0027]);

performing the authentication processing to the outputted data blocks of B2 bits in parallel to the encryption processing or the decryption processing, and outputting the authentication value indicating the result of the authentication processing (Matthews [0029]);

receiving the encrypted or decrypted data blocks, receiving the outputted authentication value, and constructing the packet including the received data blocks and the authentication value (Matthews [0026]).

wherein when the inputted packet is a packet which requires both encryption processing and authentication processing, the encryption processing of a first data block by said at least one encryption processing unit, and the authentication processing of a second data block by said at least one authentication unit are performed in parallel, the second data block to which the authentication processing is being performed being a data block which is different from the first data block and to which the encryption processing has already been performed by said at least one encryption unit and accumulated in said accumulating of the encrypted data blocks (Matthews [0029-0031]).

As per **claim 19**, Matthews discloses judging whether the inputted packet is a first type packet requiring the encryption processing and the authentication

processing, a second type packet requiring the decryption processing and the authentication processing, a third type packet requiring only one of the encryption processing and the decryption processing, or a fourth type packet requiring the authentication processing only, and when it is judged to be the first type packet, controlling so that the division in the dividing step, the encryption processing in the encryption processing step, the accumulation in the data block accumulating step, the authentication processing in the authentication processing step and the construction in the packet constructing step are performed (Matthews [0011] reference 'distinguishes portions of non-pre-padded network security protocol packet requiring one and/or another operation - authentication and/or encryption" to permit single pass processing of data).

As per **claim 20**, Matthews discloses wherein said data path connection switching unit is operable to switch a data path between two of said control unit, said at least one encryption processing unit, said at least one authentication processing unit and said at least one data block accumulation unit, so that only packets A pass through said at least one data block accumulation unit and only packets B bypass said at least one data block accumulation unit, the packets A being packets which requires both encryption processing and authentication processing and a packet which requires both decryption processing and authentication processing and a packet which requires both decryption processing and authentication processing, and the packets B being a packet which requires only encryption processing, a packet which requires only

decryption processing and a packet which requires only authentication processing (Fig 3, [0024], [0029], [0032-0035]).

As per **claim 21**, Matthews discloses wherein the data blocks are saved from said at least one encryption processing unit and said at least one authentication processing unit into said processing data saving unit, and the saved data blocks are restored from said processing data saving unit to the said at least one encryption processing unit and said at least one authentication processing unit, via said at least one data block accumulation unit ([0032]).

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 3, 4, 7, 8, 10-12, 14-16 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matthews as applied to claims 1, 2, 5, 6, 9, 13, and 17-21 above, and further in view of Videcrantz et al. (U.S. Patent No. 6,275,588).

As per **claim 3**, Matthews discloses the security communication packet processing apparatus according to Claim 1.

Matthews fails to teach wherein the number of at least one of said at least one encryption processing unit and said at least one authentication unit is two or

more, and the number of the data block accumulation unit is equal to the number of encryption processing unit.

Videcrantz discloses a security communication packet processing apparatus including a plurality of encryption processing units and authentication processing units wherein the number of accumulation units is equal to that of the encryption processing units (see Figure 11b).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Matthews the plurality of units as described in Videcrantz to remove queuing delays resulting from a plurality of packets attempting to utilize the units at the same time.

As per **claim 4**, Matthews discloses the security communication packet processing apparatus according to Claim 3.

Matthews fails to teach wherein said control unit is operable to specify, among two or more encryption processing units or two or more authentication processing units, said encryption processing unit or said authentication processing unit that is ready for processing, and output the data blocks to the specified encryption processing unit or the authentication processing unit.

Videcrantz discloses a security communication packet processing apparatus including a plurality of processing units and authentication units wherein the control unit specifies which processing unit is to be utilized (see Figure 11b).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Matthews a control unit with the capabilities

to determine which processing units have completed their calculations and are ready to output to the next processing unit as described in Videcrantz to in order to maintain order and expedite the time necessary to deal with incoming packets.

As per **claim 7**, Matthews discloses the security communication packet processing apparatus according to Claim 6.

Matthews fails to teach wherein the number of at least one of the encryption processing unit and said at least one authentication unit is two or more, and the number of the said at least one data block accumulation unit is equal to the number said at least one encryption processing unit.

Videcrantz discloses a security communication packet processing apparatus including a plurality of encryption processing units and authentication processing units wherein the number of accumulation units is equal to the number of said at last one encryption processing units (see Figure 11b).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Matthews the plurality of units as described in Videcrantz to remove queuing delays resulting from a plurality of packets attempting to utilize the units at the same time.

As per **claim 8**, Matthews discloses the security communication packet processing apparatus according to Claim 7.

Matthews fails to teach wherein the control unit is operable to specify, among two or more encryption processing units or two or more authentication processing units, said at least one encryption processing unit or said at least one authentication processing unit that is ready for processing, and output the data

blocks to the specified at least one encryption processing unit or the authentication processing unit.

Videcrantz discloses a security communication packet processing apparatus including a plurality of processing units and authentication units wherein the control unit specifies which processing unit is to be utilized (see Figure 11b).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Matthews a control unit with the capabilities to determine which processing units have completed their calculations and are ready to output to the next processing unit as described in Videcrantz to in order to maintain order and expedite the time necessary to deal with incoming packets.

As per **claim 10,** Matthews discloses the security communication packet processing apparatus according to claim 9, wherein the control unit is operable to specify the processing unit that is performing the processing of the data blocks of the packet with the lowest priority among the processing units, and after suspending the processing of the data blocks in the processing unit and saving the data blocks which were being processed in the processing unit into said processing data saving unit provided to the processing unit performing the processing of the date blocks of the packet with the lowest priority, make the processing unit perform the processing of the data blocks of the inputted packet (Matthews [0035]).

As per **claim 11**, the combined apparatus of Matthews and Videcrantz discloses a data path connection switching unit operable to connect the output of

the control unit and the input of said at least one encryption processing unit, the output of said control unit and the input of said at least one authentication processing unit, the output of said at least one encryption processing unit and the input of said at least one data block accumulation unit, and the output of said at least one data block accumulation unit and the input said at least one authentication processing unit, respectively and independently (Matthews [0024]).

As per **claim 12**, Matthews discloses the security communication packet processing apparatus according to Claim 11.

Matthews fails to teach wherein the number of at least one of the encryption processing unit and the authentication unit is two or more, and the number of the data block accumulation unit is equal to the number of said at least one encryption processing unit.

Videcrantz discloses a security communication including a plurality of encryption processing units and authentication processing units wherein the number of accumulation units is equal to the number of said at least one encryption processing units (see Figure 11b).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Matthews the plurality of units as described in Videcrantz to remove queuing delays resulting from a plurality of packets attempting to utilize the units at the same time.

As per **claim 14,** the combined apparatus of Matthews and Videcrantz discloses the security communication packet processing apparatus according to

Claim 13, wherein the control unit is operable to specify, among the processing units, the processing unit that is performing the processing of the data blocks of the packet with the lowest priority, and after suspending the processing of the data blocks in the processing unit and saving the data blocks which were being processed in the processing unit in said processing data saving unit provided to the processing unit performing the processing of the data blocks of the packet with the lowest priority, make the processing unit perform the processing of the data blocks of the inputted packet (Matthews [0035]).

As per **claim 15**, the combined apparatus of Matthews and Videcrantz discloses the security communication packet processing apparatus according to Claim 14 further comprising a data path connection switching unit operable to connect the output of said control unit and the input of said at least one encryption processing unit, the output of said control unit and the input of said at least one authentication processing unit, the output of said at least one encryption processing unit and the input of said at least one data block accumulation unit, and the output of said at least one data block accumulation unit and the input of said at least one authentication processing unit, respectively and independently (Matthews [0024]).

As per **claim 16**, Matthews discloses the security communication packet processing apparatus according to Claim 15.

Matthews fails to teach wherein the number of at least one of the encryption processing unit and the authentication unit is two or more, and the

number of the data block accumulation unit is equal to the number of said at least one encryption processing unit.

Videcrantz discloses a security communication packet processing apparatus including a plurality of encryption processing units and authentication processing units wherein the number of accumulation units is equal to the number of said at least one encryption processing units (see Figure 11b).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Matthews the plurality of units as described in Videcrantz to remove queuing delays resulting from a plurality of packets attempting to utilize the units at the same time.

As per **claim 22,** the combined apparatus of Matthews and Videcrantz discloses the security communication packet processing apparatus according to claim 12, wherein said control unit is further operable to make another processing unit read the data blocks from said processing data saving unit and restart the processing, the another processing unit having a function equivalent to a function of the processing unit performing the processing of the data blocks of the packet with the lowest priority, from which processing unit the data blocks are saved into said processing data saving unit (Matthews [0035]).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

TT/ELM

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER